2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace

Peter Z. Stockburger
Dentons US LLP
San Diego, California, USA
peter.stockburger@dentons.com

Abstract: The international principle of "due diligence" is well recognized under international law, and is an outgrowth of the general obligation of States to "do no harm". The due diligence principle imposes an obligation on States to take affirmative action to ensure their territory or objects over which they maintain sovereign control are not used for internationally wrongful purposes. The due diligence principle has been recognized by international scholars and jurists since the early 20th century, and has been adopted as a principle of customary international law in the international environmental law context by States and courts, including the International Court of Justice. The International Court of Justice has specifically endorsed a procedural aspect of due diligence – that States must conduct environmental impact assessments, where appropriate, as a precautionary measure to ensure their territory is not used for internationally wrongful purposes. In 2013 and 2017, the Tallinn Manual and Tallinn Manual 2.0 confirmed the due diligence principle applies in cyberspace. However, in both manuals, the experts could not agree on the scope of its application. And, in 2017, the Tallinn Manual 2.0 experts agreed that the due diligence obligation does not include a preventive feature, as is reflected in international environmental law. This paper examines this grey area of international law, and whether and to what extent the

precautionary principle, as adopted in the international environmental law context, could be applied in cyberspace. After an examination of the precautionary principle as applied, this paper argues its application in cyberspace would help crystallize the due diligence principle from a grey zone in international law into customary international law of cyberspace by introducing a procedural due diligence requirement for States to conduct a cyber impact assessment where appropriate.

Keywords: *due diligence, cyber due diligence*

1. INTRODUCTION

The principle of State sovereignty is considered "the most fundamental" principle of all international law,[1] and has been defined as the "supreme authority of every [S]tate within its territory"[2] to exert "independence" over the "functions of a State" to the "exclusion of any other State".[3] This principle, however, is not without limit. A number of "principles and rules of conventional and customary international law derive from the general principle of sovereignty",[4] including the "corollary"[5] principle of non-intervention, which is codified at Article 2 of the United Nations (UN) Charter and restricts States from unlawfully interfering against the territorial integrity or political independence of another State.[6] The principle of non-intervention therefore restricts States in their exercise of sovereignty from using their territory or objects over which they maintain sovereign control for purposes "detrimental to the rights of other States."[7] This specific obligation is often referred to as the duty to not commit transboundary harm,[8] and is well reflected in the writings of Oppenheim as early as 1912,[9] the 1928 *Island of Palmas* award,[10] and in the International Court of Justice's (ICJ or Court) 1949 *Corfu Channel* judgment.[11]

1 Michael Schmitt, Grey Zones in the International Law of Cyberspace, 42 Yale J. of Int'l L. Online 1, 4 (2017).
2 Lassa Oppenheim, Oppenheim's International Law, at 564 (Robert Jennings & Arthur Watts eds., 9th edn, 1992).
3 *Island of Palmas (Neth. v. U.S.)*, 2 RIAA 829, 838 (Perm. Ct. Arb. 1928) (hereinafter, *"Island of Palmas"*).
4 Int'l Group of Experts, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 11 (Rule 1) (Michael N. Schmitt ed., 2017) (hereinafter, "Tallinn Manual 2.0").
5 *Military and Paramilitary Activities in and against Nicaragua (Nicar. V. U.S.)*, 198 I.C.J. 14, 106 (June 27) (hereinafter, *"Nicaragua"*).
6 *Ibid*.; U.N. Charter Art. 2(4).
7 Schmitt, note 1, at 11.
8 Stephen Fietta et al., The South China Sea Award: A Milestone for International Environmental Law, The Duty of Due Diligence and The Litigation of Maritime Environmental Disputes? 29 Geo. Envtl. L. Rev. 711, 723 (2017).
9 Lassa Oppenheim, International Law: A Treatise, 243-44 (2nd edn, 1912).
10 *Island of Palmas*, note 3, at 829-90.
11 *Corfu Channel (U.K. v. Alb.)*, 1949 I.C.J. 4, 22 (Apr. 9) (hereinafter, *"Corfu Channel"*).

To carry out this prohibition against transboundary harm, and by extension the principle of non-intervention, States have agreed to carry out their activities with "due diligence." The due diligence obligation imposes an independent duty on States to take affirmative action to stop or prevent their territory, or the items or persons within their jurisdictional control, from knowingly being used to cause internationally wrongful acts.[12] This principle is well established "in the rules, and interpretation thereof, of numerous specialised regimes of international law[,]"[13] most notably in international environmental law. In 2010, the ICJ affirmed the principle of due diligence as reflective of customary international law in its *Case Concerning Pulp Mills on the River Uruguay* between Argentina and Uruguay (*Pulp Mills*) judgment[14] wherein the Court endorsed a preventive interpretation of the principle as "a customary rule"[15] and made clear that a State is "obliged to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State".[16] The ICJ specifically recognized States have a procedural due diligence obligation to conduct an environmental impact assessment (EIA) "before embarking on an activity having the potential adversely to affect the environment of another State[.]"[17] This principle, generally known as the precautionary principle in international environmental law, requires States to take preventive measures even in the absence of scientific certainty. The principle was further endorsed by the ICJ in its 2015 judgment in the case concerning the *Construction of a Road in Costa Rica Along the San Juan River* between Nicaragua and Costa Rica (Costa Rica).[18]

Whether and to what extent the due diligence principle, and the precautionary principle, apply in cyberspace has been the subject of extensive debate over the past five years.[19] In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) commissioned an independent group of experts (IGE) to examine whether and to what extent general principles of international law apply in cyberspace.[20] The IGE produced two manuals in response - the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual 1.0")* and the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations ("Tallinn Manual 2.0")*.[21] In both, the IGE endorsed the application of the due diligence principle in

12 *Ibid*.
13 Tallinn Manual 2.0, note 1, at 30, Rule 6, ¶1.
14 *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, 2010 I.C.J. 14, 55-56 (Apr. 20, 2010) (hereinafter, *"Pulp Mills"*); *Corfu Channel*, note 11, at 22.
15 *Pulp Mills*, note 14, at 55.
16 *Id*. at 55-56.
17 *Id*. at 83.
18 *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, 2015 I.C.J. 665, 706-707 (Dec. 16, 2015) .
19 Schmitt, note 1, at 11; Tallinn Manual 2.0, note 4, at 30 (Rule 6).
20 Tallinn Manual 2.0, note 4, at 1.
21 Int'l Group of Experts, Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013) (hereinafter, "Tallinn Manual 1.0"); Tallinn Manual 2.0, note 4.

cyberspace,[22] but could not agree on its scope.[23] In the 2017 *Tallinn Manual 2.0*, for example, the IGE agreed the due diligence principle applies in cyberspace,[24] but was "divided as to the interpretation of the due diligence obligation".[25] Specifically, the IGE agreed the principle generally applies when cyber operations "having serious adverse consequences vis-à-vis a legal right of a State are mounted from another State's territory",[26] but could not agree that there was a preventive or precautionary element tied to this obligation.[27] The IGE also noted that because "not every State involved in pre-publication consultations readily accepted the application of due diligence to cyberspace as a matter of customary law", there was a view, not shared by the IGE, "by which the premise of applicability is *lex ferenda* (what the law should be), rather than *lex lata* (current law)".[28] This view, according to the IGE, appears to be based in part on the 2013 and 2015 reports of the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Informational Security (GGE),[29] which only agreed that States "should," rather than must, take actions necessary to put an end to cyber operations emanating from their territory which are harmful to other States.[30]

This paper examines this grey area of international law, and whether a preventive or precautionary principle should, as the *lex ferenda*, apply in cyberspace. This paper specifically explores whether applying a procedural due diligence requirement in cyberspace, similar to the procedural due diligence obligation in environmental law, would help crystallize the due diligence obligation in cyberspace and close the gap recognized by the *Tallinn Manual 2.0.* In so doing, this paper argues that States should agree to conduct a cyber impact assessment as a procedural due diligence requirement that each would undertake before embarking on an activity having the potential adversely to affect the cyber infrastructure or interests of another State. This principle, of course, is not the *lex lata*. States have not agreed to this approach in cyberspace. But because there are analogies to be drawn between significant and irreparable environmental harm and the harm that a serious and adverse cyber operation could impose on States, this paper argues the *lex ferenda* should properly consider the application of a precautionary approach in cyberspace to further ensure States have clear rules concerning due diligence in their cyber operations vis-à-vis one another.

22 Tallinn Manual 1.0, note 22, at 26.
23 *Id*. at 28.
24 Schmitt, note 1, at 11; Tallinn Manual 2.0, note 4, at 30 (Rule 6).
25 Schmitt, note 1, at 11.
26 *Ibid*.
27 *Id*. at 13; Tallinn Manual 2.0, note 4, at 41-42 (Rule 6) cmt. 42; *id*. at 44-45 (Rule 7) cmts. 7-10.
28 Schmitt, note 1, at 11; Tallinn Manual 2.0, note 4, at 31 (Rule 6) cmt. 3.
29 Schmitt, note 1, at 11.
30 Rep. of the Grp. of Governmental Experts on Devs. In the Field of Info. & Telecomm. In the Context of Int'l Sec., U.N. Doc. A/68/98, ¶ 23 (June 24, 2013) (hereinafter, "2013 GGE Report"); Rep. of the Grp. of Governmental Experts on Devs. In the Field of Info. & Telecomm. In the Context of Int'l Sec., U.N. Doc. A/70/174, ¶¶ 13(c), 28(e) (July 22, 2015) (hereinafter, "2015 GGE Report").

This paper is divided into four parts. **Part I** examines the history of the due diligence principle as it has developed under international law. **Part II** examines the development of the precautionary approach in international environmental law. **Part III** examines the application of the due diligence principle in cyberspace, as reflected in the *Tallinn Manual 1.0, Tallinn Manual 2.0*, and the 2013 and 2015 GGE Reports. And **Part IV** explores how, if adopted, a precautionary approach may help further crystallize due diligence in cyberspace by imposing a procedural due diligence obligation on States.

2. PART I - DEVELOPMENT OF DUE DILIGENCE UNDER INTERNATIONAL LAW

The obligation of "due diligence" is well recognized in international law, and dates back to the writings of Grotius and Vattel.[31] The principle has been applied in various specialized regimes of international law, including international human rights, humanitarian, trade, and environmental law.[32] The ICJ expressly endorsed the due diligence principle in its 1949 *Corfu Channel* judgment, stating there are "certain general and well-recognized principles" of international law, including "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[33] The ICJ further endorsed the principle in the case concerning the *Prevention and Punishment of the Crime of Genocide*.

In addition to these general developments, the principle of due diligence has received considerable attention in the international environmental context. It was first endorsed in the 1938 *Trail Smelter* Arbitral Award, which determined that Canada was required to take protective measures to reduce the air pollution in the Columbia River Valley caused by sulphur dioxide emitted by zinc and lead smelter plants in Canada, only seven miles from the Canadian-US border:[34]

> Under the principles of international law, no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence.[35]

The ICJ further endorsed this principle in 2010 and 2015, and introduced the preventive principle within the due diligence obligation in the *Pulp Mills* and *Costa*

31 Stephen Fietta, et al., The South China sea Award: A Milestone for International Environmental Law, The Duty of Due Diligence and The Litigation of Maritime Environmental Disputes? 29 Geo. Envtl. L. Rev. 711, 723 (2017).

32 Fietta, note 32, at 723 (citing Friendly Relations Declaration, multiple Security Council resolutions, the four Geneva Conventions of 1949, and multiple arbitral decisions).

33 *Corfu Channel*, note 11, at 22.

34 *Trail Smelter (U.S. v. Can.)*, 3 R.I.A.A. 1905, 1965 (1938).

35 *Ibid*.

Rica judgments. In its 2010 *Pulp Mills* judgment, the ICJ affirmed the principle of due diligence as reflective of customary international law, and relied on its articulation of the principle in its 1949 *Corfu Channel* judgment.[36] From this general principle, the ICJ additionally recognized that within the due diligence principle there exists a principle of prevention which is also "a customary rule",[37] and obliges States to "use all the means at [their] disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State".[38] The ICJ made clear in its judgment that it may now be considered a requirement under general international law to undertake an environmental impact assessment where there is a risk that the proposed industrial activity may have a significant adverse impact in a transboundary context, in particular, on a shared resource.[39]

Although the Court's judgment in *Pulp Mills* referred only to industrial activities, the Court further expanded on the principle in its 2015 *Costa Rica* judgment and affirmed the principle of due diligence and that the requirement of an EIA "applies generally to proposed activities which may have a significant adverse impact in a transboundary context".[40] The Court stated that in order to "exercise due diligence in preventing significant transboundary environmental harm, a State must, before embarking on an activity having the potential adversely to affect the environment of another State, ascertain if there is a risk of significant transboundary harm, which would trigger the requirement to carry out an environmental impact assessment.[41] This principle, the preventive principle, is also known as the precautionary principle.

3. PART II - DEVELOPMENT OF PRECAUTIONARY PRINCIPLE

A. 1971 - 1991

Most commentators agree that the "precautionary" principle traces back to 1971 and the concept of *Vorsorgeprinzip* (foresight) under German environmental law.[42] This principle was asserted by Germany ten years later during international conferences held to discuss the protection of the North Sea,[43] and was adopted in 1987 as part of the Ministerial Declaration Calling for Reduction of Pollution, which stated in relevant part:

36 *Pulp Mills*, note 14, at 55-56; *Corfu Channel*, note 11, at 22.
37 *Pulp Mills*, note 14, at 55.
38 *Id*. at 55-56.
39 *Id*. at 83.
40 *Costa Rica*, note 18, at 706.
41 *Id*. at 706-707.
42 Ling Chen, Realizing the Precautionary Principle in Due Diligence, 25 Dal. J. Leg. Stud. 1, 4 (2016); Mary Stevens, The Precautionary Principle in the International Arena, 2 Sus. Dev. Law & Pol. 13, 13 (2002).
43 Stevens, note 42, at 13.

> [in] order to protect the North Sea from possibly damaging effects of the most dangerous substances, a precautionary approach is necessary which may require action to control inputs of such substances even before a causal link has been established by absolute clear scientific evidence.[44]

The principle was also referenced in the 1987 Montreal Protocol on Substances that Deplete the Ozone Layer, which provides that States must "protect the ozone layer by taking precautionary measures to control equitably total global emissions that deplete it".[45]

By 1990, the principle had received widespread adherence. It was applied at the third conference on the protection of the North Sea[46] and was also included in Great Britain's 1990 White Paper on Britain's Environmental strategy, which provided:

> We must analyze the possible benefits and costs both of action and of inaction. Where there are significant risks of damage to the environment, the Government will be prepared to take precautionary action to limit the use of potentially dangerous pollutants, even where scientific knowledge is not conclusive, if the balance of the likely costs and benefits justifies it. This precautionary principle applies particularly where there are good grounds for judging either that action taken promptly at comparatively low cost may avoid more costly damage later, or that irreversible effects may follow if action is delayed.[47]

Europe further endorsed the principle in 1991 in a meeting between parties to the 1927 London Dumping Convention,[48] and in the Bamako Convention of 1991 which requires States party to prevent the "release into the environment of substances which may cause harm to humans or the environment without waiting for scientific proof regarding such harm".[49]

B. 1992 To The Present

The precautionary principle gained momentum in 1992, and was endorsed in multiple international instruments, including Article 2 of the 1992 Convention for the

44 Chen, note 42, at 5.

45 *Montreal Protocol on Substances that Deplete the Ozone Layer*, 16 September 1987, 1522 UNTS 3 (entered into force 1 January 1989).

46 Final Declaration of the Third International Conference on Protection of the North Sea, Mar. 7-8, 1990. 1 YB Int'l Envtl Law 658, 662-73 (1990).

47 This Common Inheritance: Britain's Environmental Strategy, Sept. 1990 at § 1.18.

48 London Dumping Convention Amendments (1991).

49 *Bamako Convention on the Ban of the Import into Africa and the Control of Transboundary Movement and the Management of Hazardous Wastes Within Africa*, Jan. 30, 1992, OAU/CONF/COOR/ENV/MIN/AFRI/CONV.1(1) Rev. 1, reprinted in 30 L.L.M. 773.

Protection of the Marine Environment of the Northeast Atlantic and Article 15 of the landmark Rio Declaration, which was signed at the UN Conference on Environment and Development and provides that:

> In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.[50]

The 1992 UN Framework Convention on Climate Change also endorsed the precautionary principle:

> The parties should take precautionary measures to anticipate, prevent, or minimize the causes of climate change and mitigate its adverse effects. Where there are threats of serious or irreversible damage, lack of full scientific certainty should not be used as a reason for postponing such measure, taking into account that policies and measure to deal with climate change should be cost-effective so as to ensure global benefits at the lowest possible cost.[51]

Article 6 of the 1995 Agreement for the Implementation of the Provisions of the 1982 UN Convention on the Law of the Sea relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks further endorsed the application of the precautionary approach,[52] and provided that States party are required to use the precautionary approach to conserve, manage, and exploit the stocks of straddling fish and highly migratory fish and "shall be more cautious when information is uncertain, unreliable or inadequate".[53] Under this principle, States cannot delay or refuse to take conservation and management measures because of inadequate scientific information.[54] States are also required to implement the precautionary principle when developing scientific information and technology to mitigate uncertainties relating to the size of fish stocks, and collect data to assess the impact of certain fishing activities.[55]

50 Rio Declaration at art. 15.
51 United Nations Framework Convention on Climate Change, May 9, 1992, art. 3, para. 3, U.N. Doc. A/CONF.151/26.
52 UNGA, Conference on Straddling Fish Stocks and Highly Migratory Fish Stocks, 6th Sess, *Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks*, UN Doc A/CONF.164/37, September 1995.
53 *Id*. at Art. 6.1, 6.2.
54 *Ibid*.
55 *Id*. at art. 6.3.

The 2000 Cartagena Protocol on Biosafety to the Convention on Biological Diversity also applies the precautionary principle to the control of transboundary movements of genetically modified organisms,[56] wherein the principle is reflected in paragraph 4 of its preamble[57] and Articles 1, 10(6) and 11(8).[58] Articles 10(6) and 11(8), both of which track precautionary language, include language such as "lack of scientific certainty", "insufficient relevant scientific information and knowledge", and the minimization of "potential adverse effects".[59]

As noted above, the ICJ embraced the precautionary principle in the 2010 *Pulp Mills* judgment, and made clear that the due diligence principle carries with it a procedural element – the undertaking of an EIA in appropriate circumstances to determine if there is a risk of significant transboundary harm, which would trigger the requirement to carry out an environmental impact assessment.[60] The Court further articulated that the content of the EIA is to be made in "light of the specific circumstances of each case":[61]

> it is for each State to determine in its domestic legislation or in the authorization process for the project, the specific content of the environmental impact assessment required in each case, having regard to the nature and magnitude of the proposed development and its likely adverse impact on the environment as well as to the need to exercise due diligence in conducting such an assessment.[62]

The Court further elaborated on this procedural due diligence obligation in the *Costa Rica* judgment, noting that if the:

> environmental impact assessment confirms that there is a risk of significant transboundary harm, the State planning to undertake the activity is required, in conformity with its due diligence obligation, to notify and consult in good faith with the potentially affected State, where that is necessary to determine the appropriate measures to prevent or mitigate that risk.[63]

56 *Cartagena Protocol on Biosafety to the Convention on Biological Diversity*, 29 January 2000, 2226 UNTS 208 (entered into force 11 September 2003).
57 *Id*. at preamble, para. 4.
58 *Id*. at arts 1, 10(6), 11(8).
59 *Id*. at art 10(6), 11(8).
60 *Costa Ric*a, note 18, at 706-07.
61 *Id*. at 707.
62 *Pulp Mills*, note 11, at 83.
63 *Costa Rica*, note 18, at 707.

4. PART III - DUE DILIGENCE IN CYBERSPACE

Whether and how the principle of due diligence and its precautionary approach apply in cyberspace has been examined closely by scholars and jurists over the past five years. Although there are myriad opinions on the application of due diligence in cyberspace, this paper focuses solely on those opinions set out in the *Tallinn Manual 1.0, Tallinn Manual 2.0*, and the 2013 and 2015 GGE Reports.

A. Tallinn Manual 1.0

The *Tallinn Manual 1.0* endorses the principle of due diligence in cyberspace by reaffirming the principle that a State may not "allow knowingly its territory to be used for acts contrary to the rights of other States".[64] The IGE concluded that States, in their cyber operations, are to "take appropriate steps to protect those rights".[65] The scope of that obligation, however, was the subject of extensive debate and disagreement. Indeed, due diligence was only dealt with in a single rule accompanied by a brief commentary. And the IGE could not achieve consensus on the parameters of the obligation. The IGE noted that the implementation of the due diligence principle in cyberspace is complicated by the nature of harmful cyber acts, "especially time and space compression, and their often-unprecedented character."[66]

The IGE therefore adopted a knowledge standard when applying the due diligence principle in cyberspace, noting that the principle of due diligence applies only if the territorial State has "actual knowledge" of the cyber operation and/or the threat in question.[67] The IGE could not "achieve consensus" as to whether the principle of due diligence applies if "the respective State has only constructive ('should have known') knowledge".[68] In other words, the IGE agreed it was:

> unclear whether a State violates [the principle of due diligence] if it fails to use due care in policing cyber activities on its territory and is therefore unaware of the acts in question. Even if constructive knowledge suffices, the threshold of due care is uncertain in the cyber context because of such factors as the difficulty of attribution, the challenges of correlating separate sets of events as part of a coordinated and distributed attack on one or more targets, and the ease with which deception can be mounted through cyber infrastructure.[69]

64 Tallinn Manual 1.0, note 22, at 26.
65 *Ibid*.
66 *Id*. at 27.
67 *Id*. at 28.
68 *Ibid*.
69 *Ibid*.

The IGE also could not agree on whether a State must take preventive measures to ensure the cyber hygiene of the infrastructure on its territory or whether "States should be required to monitor for malicious activity that might be directed at other States".[70]

B. Tallinn Manual 2.0

The Tallinn Manual 2.0 further confirmed that the due diligence principle applies to cyber operations originating from a State's territory,[71] making clear that the principle of due diligence was reflected in international law and applied in cyberspace as the *lex lata*.[72] Notwithstanding, the IGE rejected the notion that due diligence in cyberspace involves an "obligation of prevention", stating that the group of experts was in agreement that the "due diligence principle does not encompass an obligation to take material preventive steps to ensure that the State's territory is not used in violation [of the law]".[73] In reaching this decision, the IGE stated it "carefully considered whether the due diligence principle imposes a requirement to take preventive measures, such as hardening one's cyber infrastructure, to reduce general, as distinct from particularised, risks of future cyber operations falling within the purview of the [due diligence principle].[74]

Ultimately, the IGE "rejected the premise of a requirement to take purely preventive measures of a general nature"[75] based on the difficulty in mounting comprehensive and effective defences against all possible cyber threats.[76] Such a requirement, according to the IGE, would "impose an undue burden on States, one for which there is no current basis in either the extant law or current State practice."[77] The IGE further noted that "States have not indicated that they believe such a legal obligation exists with respect to cyber operations, either by taking preventive measures on this basis or by condemning the failure of other States to adopt such measures".[78]

The IGE also noted that because knowledge is a requirement under the principle of due diligence, it would be "contradictory to expand" the principle of due diligence to "hypothetical future cyber operations"[79] because a State cannot know of a "cyber operation that has yet to be decided upon by the actor".[80] Thus, having rejected the duty of prevention, the IGE concurred that a State is "not required to monitor cyber activities on its territory".[81]

70 Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, The Yale Law Journal Forum at 71 (June 22, 2015).
71 Tallinn Manual 2.0, note 4, at 30 (Rule 6).
72 *Id*. at 31 (Rule 6). The IGE also acknowledge a view, which no member held, that the due diligence principle is not reflective of custom based on the non-mandatory language found in the 2013 and 2015 GGE Reports.
73 *Id*. at 32 (Rule 7).
74 *Id*. at 44.
75 *Ibid*.
76 *Id*. at 45.
77 *Ibid*.
78 *Ibid*.
79 *Id*. at 45.
80 *Ibid*.
81 *Ibid*.

The IGE, did, however, acknowledge the precautionary approach in international law. It "acknowledged the contrary view, which none of them held, that the due diligence obligation extends to situations in which the relevant harmful acts are merely possible".[82] "By it, States must take reasonable measures to prevent them from emanating from their territory."[83] The IGE notes that this view is based on the existence of an obligation to "take preventive measures in the context of transboundary environmental harm".[84] According to this position, a "State must take feasible preventive measures that are proportionate to the risk of potential harm. They have to take account of technological and scientific developments, as well as the unique circumstances of each case".[85]

The IGE rejected this principle, practically, because "if such an approach were to be adopted, it would be unclear when the obligation would be breached":

> One possibility is that a breach takes place when a target State is placed at the risk of harm by virtue of the territorial State not having taken appropriate measures to prevent harmful cyber operations being mounted from or through its territory. Another is that although the due diligence principle requires States to take appropriate preventive measures, they cannot be held responsible for having failed to do so unless and until the target State actually suffers the requisite harm.[86]

The IGE concluded that the "precise threshold of harm at which the due diligence principle applies is unsettled in international law".[87]

C. The 2013 and 2015 GGE Reports

In 2013, the UN GGE issued a report on the application of "norms derived from existing international law relevant to State behavior in cyberspace".[88] Concerning the due diligence principle, the GGE concluded that States must "meet their international obligations regarding internationally wrongful acts attributable to them", and "should seek to ensure that their territories are not used by non-State actors for unlawful use" of their cyber infrastructure.[89] In 2015, the GGE reaffirmed this principle, and stated that "States should not knowingly allow their territory to be used for internationally wrongful acts" using their cyber infrastructure.[90] The use of the word "should" instead of "shall" or "must" has raised questions as to whether States truly understand that

82 *Ibid*.
83 *Ibid*.
84 *Id*. at 45-46.
85 *Id*. at 46.
86 *Ibid*.
87 Tallinn Manual 2.0, note 4, at 36.
88 2013 GGE Report, note 31, at 2.
89 *Id*. at 8, ¶23.
90 2015 GGE Report, note 31, at 8, ¶13(c)

the due diligence principle is reflective of customary international law. "[As] due diligence is purportedly a primary rule of international law, a State's violation of which constitutes an internationally wrongful act, such hesitancy to accord the rule lex lata status produces a grey zone of international law."[91]

5. ADOPTING THE PRECAUTIONARY APPROACH IN CYBER

Whether the due diligence obligation reflects the *lex lata* in cyberspace is not the focus of this paper. This paper instead questions the 2017 *Tallinn Manual 2.0* IGE's conclusion that a preventive feature of due diligence cannot apply in cyberspace. The 2017 IGE rejected the application of the precautionary approach in cyberspace because States cannot harden their cyber defenses against all possible cyber threats.[92] The IGE also rejected its application because knowledge is a requirement to trigger the due diligence principle, and it would be "contradictory to expand" the principle of due diligence to "hypothetical future cyber operations" because a State cannot know of a "cyber operation that has yet to be decided upon by the actor".[93]

These are legitimate concerns. However, they would be mitigated if States adopted a procedural due diligence obligation, similar to the standard articulated by the ICJ in the 2010 *Pulp Mills* and 2015 *Costa Rica* judgments. In particular, a procedural due diligence approach in cyberspace would not require States to harden their systems against any possible cyber threat. Nor would it require States to guard against any "hypothetical future cyber operations". Instead, as the Court stated in *Pulp Mills* and *Costa Rica*, States would have a procedural due diligence obligation that would be triggered once the State embarks on any activity "having the potential adversely to affect the [rights and interests] of another State" to "ascertain if there is a risk of significant transboundary harm".[94] Specifically, in such circumstances, States would be required to conduct an "impact assessment" to determine if the State's actions in cyberspace would have the potential to adversely affect the rights and interests of another State.

This "impact assessment" could come in a variety of forms and would be circumscribed in "light of the specific circumstances of each case".[95] For example, as the Court noted in *Pulp Mills*, it would be for "each State to determine in its domestic legislation" the specific content of the impact assessment required in each case, having regard to "the nature and magnitude" of the proposed activity and its likely adverse impact on the

91 Schmitt, note 1, at 11.
92 *Id*. at 45.
93 *Ibid*.
94 *Costa Rica*, note 18, at 706-07.
95 *Id*. at 707.

rights and interests of other States, "as well as to the need to exercise due diligence in conducting such an assessment".[96] Further, as the Court stated in *Costa Rica*, if the impact assessment "confirms that there is a risk of significant transboundary harm, the State planning to undertake the activity is required, in conformity with its due diligence obligation, to notify and consult in good faith with the potentially affected State, where that is necessary to determine the appropriate measures to prevent or mitigate that risk".[97]

Adopting the preventive / precautionary approach in cyberspace would therefore introduce a procedural due diligence obligation on States, and would impose two distinct obligations on States. First, if the State plans to engage in activity having the potential adversely to affect the rights and interests of another State, the State would undertake a cyber impact assessment to ascertain if there is a risk of significant transboundary harm resultant from that action. Second, if the impact assessment confirms there is a risk of significant transboundary harm, the State planning to undertake the activity is required, in conformity with its due diligence obligation, to notify and consult in good faith with the potentially affected State, where that is necessary to determine the appropriate measures to prevent or mitigate that risk.

Adopting this obligation is not impossible for States, as many already implement the due diligence principle in many of their cyber strategies and domestic plans. In its 2011 International Strategy for Cyberspace, for example, the United States stated that "States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse".[98] Germany likewise adopted a due diligence approach in many of its national programs and strategies.[99] Similar jurisdictions have due diligence principles built into their programmes, including new data protection regulations in the European Union.

Adopting a procedural due diligence approach in cyberspace would also be consistent with international law. States are already bound to conduct their international relations with other States in "good faith,"[100] which has been defined as a sustained upkeep of negotiations over a period appropriate to the circumstances and with an awareness of the interests of the other party.[101] States could apply this principle when determining whether to enter into negotiations with other States regarding the results of their impact

96 *Pulp Mills*, note 11, at 83.
97 *Costa Rica*, note 18, at 707.
98 International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, White House 10 (2011).
99 Annegret Bendiek, *Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy*, SWP Research Paper at 22 (2016).
100 Rogoff, *The Obligation to Negotiate in International Law: Rules and Realities*, 16 Mich, J. Int'l L. 141, 153 (1994).
101 *Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Georgia v. Russian Federation)*, 2011 I.C.J. 157 (2011); *Arbitration between Kuwait and the American Independent Oil Co., (AMINOIL)* 21 ILM 1982, 1014; *Lac Lanoux Arbitration (France v. Spain)* (1957) 24 I. L. R. 101, 23 November 16, 1957.

assessment, and whether certain systems should be hardened, or further information should be exchanged.

Adopting a procedural due diligence approach in cyberspace would also address the underlying concern addressed in international environmental law – the prevention of significant and non-reversible transboundary harm. Over the past ten years alone, from the 2007 attack in Estonia to the 2016 attack in the United States, the scope and impact of detrimental cyber operations has been manifest. The precautionary principle would require an impact assessment be conducted, even if technical certainty is not conclusive to prevent transboundary harm. In this context, applying the precautionary approach in cyberspace would not, as the IGE supposes in the *Tallinn Manual 2.0*, place an unreasonable burden on States, because the obligation would not require the State to harden systems *per se* but only to conduct a procedural review to determine if there is a threat of significant harm to another State. Thus, under the formulation set out by the ICJ in the *Pulp Mills* and *Costa Rica* cases, the precautionary approach in cyberspace could blend procedural and substantive elements.

From a substantive perspective, it could be agreed between States that, as a general rule, States must take steps to mitigate any potential transboundary harm resultant from potential cyber operations using that territorial State's cyber infrastructure, even if there is no conclusive evidence of attribution, technical identification, or operational certainty. To effectuate this substantive obligation, as in the environmental context, a procedural obligation would be required by States that would place a lesser burden on them. This requirement would not, as the 2017 IGE suggests, require a State to anticipate every hypothetical attack. It would instead allow the territorial State to understand the current state of its national cyber infrastructure, to measure that against known threats within and outside its jurisdiction, and to make a determination as to whether it should consult with other States based on a threat analysis commensurate with the experience and resources of the territorial State. As the ICJ noted in *Costa Rica*, the scope and substance of such an assessment would be subject to the circumstances of each State.

Of course, there are certain guideposts that could be established by treaty that would outline the scope of any such impact assessment. States could agree, for example, that when triggered a general framework for review should be used similar to that provided in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[102] This uses a common language to address and manage cybersecurity risk for private business, focusing on a risk management framework. Many private-sector entities understand that the standard for private sector "due diligence" is compliance with the NIST Framework[103] and several

102 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (2014) (hereinafter, "NIST Framework").

103 Why the NIST Cybersecurity Framework Isn't Really Voluntary, Info. Sec. Blog (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

States are engaged in NIST collaborations, including the United Kingdom, Japan, Korea, Estonia, Israel, and Germany.[104] In any event, this paper does not endorse any particular method of impact assessment, only that once triggered, States should agree that conducting an impact assessment is a procedural due diligence requirement.

By segregating procedural and substantive due process, the concern raised by the IGE in *Tallinn Manual 2.0* that the due diligence principle is difficult to effectuate in cyber space because of the "difficulty of mounting comprehensive and effective defences against all possible cyber threats"[105] would be mitigated. States would not have to mount comprehensive and effective defenses against all possible cyber threats. Territorial States would instead only need to conduct a procedural due diligence impact assessment, if triggered. In *Pulp Mills*, the ICJ noted that the scope and substance of EIAs would be dependent on the specific "nature and magnitude of the proposed development and its likely adverse impact on the environment".[106] Likewise in cyber, the scope and nature of an impact assessment would be dependent on the nature and magnitude of the particular cyber infrastructure in question. For example, an impact assessment conducted by the United States or China would be significantly more complex than that conducted of lesser cyber capable States. The standards could be flexible. But the underlying principle should be clear.

By adopting the precautionary approach, as reflected in the ICJ's jurisprudence, States would have a clear obligation that would help better crystallize the substantive due diligence obligation that has evaded State interest to date.

6. CONCLUSION

The IGE recognized in the *Tallinn Manual 2.0* that "in light of the nature of cyber activities, preventive measures are arguably prudent".[107] Applying the precautionary approach to the due diligence principle in cyberspace would help to crystallize the principle of due diligence, and encourage increased adherence, by implementing a prudent and understandable procedural obligation. The precautionary principle in cyberspace is, of course, not reflective of customary international law. This paper argues that instead the approach is the *lex ferenda*, or where the law should go. The benefits of the precautionary approach, especially delineating between procedural and substantive due diligence, would have clear benefits in cyberspace by providing more clear guideposts for States on what is required when carrying out due diligence. By requiring States to undergo critical assessments of their cyber infrastructure to

104 See Brian Fung, *A Court Just Made It Easier for the Government to Sue Companies for Getting Hacked*, Wash. Post (Aug. 24, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/08/24/a-court-just-made-it-easier-for-the-government-to-sue-companies-for-getting-hacked/?wpmm=1&wpisrc=nl_headlines.

105 Tallinn Manual 2.0 at p. 45, Rule 6, ¶ 8.

106 *Pulp Mills*, note 11, at ¶205.

107 Tallinn Manual 2.0, note 4, at 46 (Rule 7).

determine potential vulnerabilities, the precautionary approach would create a baseline obligation for States that could help to crystallize the due diligence principle in cyberspace, and help move this grey zone of international law to a principle of customary international law.